FortiClient (Mac OS X) - Release Notes

VERSION 5.4.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

October 09, 2015

FortiClient (Mac OS X) 5.4.0 Release Notes

04-540-290938-20151009

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-10-09	Initial release.
2016-03-17	Added 294213, 309575, and 298065 to Known Issues.

Introduction

This document provides a summary of enhancements, support information, and installation instruction for FortiClient (Mac OS X) 5.4.0 build 0493.

This document includes the following sections

- Introduction
- What's New in FortiClient (Mac OS X) 5.4.0
- Installation Information
- Product Integration and Support
- Resolved Issues
- Known Issues

Please review all sections prior to installing FortiClient. For more information, see the *FortiClient Administration Guide* in the Fortinet Document Library.

Licensing

FortiClient offers two licensing modes:

- Standalone Mode
- Managed Mode

Standalone Mode

In standalone mode, FortiClient is not registered to a FortiGate or Enterprise Management Server (EMS). In this mode, FortiClient is free both for private individuals and commercial businesses to use. No license is required. All features and functions are activated.

Managed Mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. This is accomplished by registering each FortiClient to a FortiGate, or to an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.

Licensing on the FortiGate or EMS is based on the number of registered clients. FortiGate 30 series and higher models support ten (10) free managed FortiClient licenses. For additional managed clients, a FortiClient license subscription must be purchased. The maximum number of managed clients varies per device model.

FortiClient Licenses on the FortiGate

The following table shows client limits per FortiGate model series.

The ability to download the license file, pre-configure the client, create a custom installer, and rebrand are included.

FortiGate Series	FortiClient License Upgrade
FortiGate/FortiWiFi 30 to 90 series	200 clients
FortiGate 100 to 300 series	600 clients
FortiGate 500 & above FortiGate vM01 w/ FOS 5.4 & above	2000 clients
FortiGate 1000 series & above FortiGate VM04 w/ FOS 5.4 & above	2000 clients 8000 clients
FortiGate 3000 & above FortiGate VM08 w/ FOS 5.4 & above	2000 clients 8000 clients 20 000 clients

Each FortiGate offers 10 free licenses by default. FortiGate 1000 and 3000 series both may use the 2000 or 8000 client license.

In high availability (HA) configurations, all cluster members require an upgrade license key.

FortiClient Licenses on the EMS

A newly installed EMS offers 20,000 trial client licenses over a period of 60 days from the day of installation. After the trail period lapses, the number of client licenses will be 10, same as for a new FortiGate to which no FortiClient license has been applied.

A license may be applied to the EMS at any time during or after the trial period. Licenses are available in multiples of 100 seats, with a minimum of 100 seats.

Special Notices

Change in FortiClient Endpoint Control Default Registration Port

FortiClient registers to the FortiGate using Endpoint Control (EC). In FortiClient 5.0 and 5.2, the default registration port is TCP port 8010. FortiOS 5.0 and 5.2 both listen on TCP port 8010.

Starting with FortiClient 5.4, EC registration will use port 8013 by default. To register to FortiOS 5.0 or 5.2, the user must specify port 8010 with the IP address, separated by a colon. For example, <ip_address>:8010.

FortiOS 5.4 will listen on port 8013. If registering from FortiClient 5.4 to FortiOS 5.4, the default ports will match. Specifying the port number with then IP address is then optional.

Support for Mac OS X 10.11 - El Capitan

FortiClient 5.4.0 supports the recently released Mac OS X 10.11, El-Capitan, along with older versions 10.8 to 10.10. All existing FortiClient features work correctly, but please review the following:

Mac OS X 10.11 introduced a new software issue in the DNS resolver. If there are two network interfaces (such as one ethernet and one WiFi), traffic may be routed into one of the interfaces, while the source IP address is set to the other interface. This flaw impacts FortiClient users when using split tunnel VPN connections. The Fortinet development team has reported the issue to Apple.

With a full VPN tunnel configuration, all traffic goes through the tunnel. There is only one source IP address. A VPN split tunnel means the operating system will see two network interfaces, one private and one public. Thus, if DNS traffic goes out with the wrong source IP address, the response will not be received.

This issue does not exist on Mac OS X 10.8 to 10.10. Users encountering this issue on Mac OS X 10.11 may:

- use a public DNS, so that all DNS traffic goes through the public interface
- use full VPN tunnels

What's New in FortiClient (Mac OS X) 5.4.0

AntiVirus

Advanced Persistent Threats

FortiClient 5.4.0 has enhanced capabilities for the detection of Advanced Persistent Threats (APT). On Mac OS X systems, Botnet Command and Control Communications Detection capabilities have been introduced.

Botnet Communication Detection

Botnets running on compromised systems usually generate outbound network traffic directed towards Command and Control (C&C) servers of their respective owners. The servers may provide updates for the botnet, or commands on actions to execute locally, or on other accessible, remote systems. When the new botnet feature is enabled, FortiClient monitors and compare network traffic with a list of known Command and Control servers. Any such network traffic will be blocked.

Web Filtering

Web Browser Usage and Duration

If configured, FortiClient will record detailed information about the user's web browser activities, such as:

- A history of websites visited by the user (as shown in regular web browser history)
- An estimate of the duration or length of stay on the website

These logs are sent to FortiAnalyzer, if configured. With FortiAnalyzer 5.4.0 (or newer) the FortiClient logs sent from various endpoints may be viewed in FortiView.

Endpoint Control

Integration with the New Enterprise Management Server

The Enterprise Management Server (EMS) is a new product from Fortinet for businesses to use to manage their computer endpoints. It runs on a Windows Server, so it does not require a physical Fortinet device. Administrators may use it to gain insight on the status of their endpoints. The EMS supports devices running Microsoft Windows, Mac OS X, Android and iOS.

FortiClient Endpoint Control protocol has been updated to seamlessly integrate with the EMS. Various changes were added to support EMS features, such as:

- Continuous monitoring of device status
- AV engine and signature update status reports
- AV scanning schedule. Requesting for AV scan
- Notifications about protection status

FortiGate Network Access Control with EMS Integration

When creating a FortiClient profile on EMS, the administrator can choose to configure the FortiClient to register to the same EMS or to a FortiGate. Changes in FortiClient 5.4.0 allow it to register to a FortiGate, while simultaneously, notifying the EMS of its registration status. The FortiClient EC registration to the FortiGate is required for Network Access Compliance (NAC). The administrator can configure the FortiGate to allow access to network resources only if the client is compliant with the appropriate interface EC profile.

This feature requires FortiOS 5.4.0 or newer.

Quarantine an Infected Endpoint from the FortiGate or EMS

A computer endpoint that is considered to be infected may be quarantined by the FortiGate or EMS (Enterprise Management Server) administrator. FortiClient needs to be registered and online, using Endpoint Control, to the said FortiGate or EMS.

Once quarantined, all network traffic to or from the infected endpoint will be blocked locally. This allows time for remediation actions to be taken on the endpoint, such as scan and clean the infected system, revert to a known clean system restore point or re-install the operating system.

The Administrator may un-quarantine the endpoint in the future from the same FortiGate or EMS.

This feature requires either FortiOS 5.4.0 or EMS 1.0.0.

Importing FortiGate CA Certificate after Endpoint Control Registration

When the FortiGate is configured to use SSL deep inspection, users visiting encrypted websites will usually receive an invalid certificate warning. The certificate signed by the FortiGate does not have a Certificate Authority (CA) at the endpoint to verify it. Users can manually import the FortiGate CA certificate to stop the error from being displayed. However, all users will have to do the same.

When registering Endpoint Control (EC) to a FortiGate, the FortiClient will receive the FortiGate's CA certificate and install it into the system store. If Firefox is installed on the endpoint, the FortiGate's CA certificate will also be installed into Firefox certificate store. Thus, the end user will no longer receive the invalid certificate error message when visiting encrypted websites.

The FortiGate CA certificates will be removed from the system store if FortiClient is uninstalled.

Enhancement on On-net/Off-net Configuration

The on-net feature requires the use of a FortiGate as the DHCP server. This is usually configured on the same FortiGate that the FortiClient will be registered. When the device on which FortiClient is running has an IP address from the FortiGate's DHCP server, it is on-net. For any other IP addresses, it is off- net.

There is a new way to configure the on-net feature. On the FortiGate, the DHCP server can be used, or several network subnets can be provided.

FortiClient will be on-net if:

- It is registered using EC to the FortiGate
- It belongs to one of the pre-configured on-net subnets, or
- It provides the DHCP for on-net properties.

Otherwise, it is off-net.

FortiClient GUI

AntiVirus Settings Page

With the introduction of botnet detection, the AV settings page on the FortiClient GUI has been updated to allow configuration of the new features. The AV settings page is accessible from the FortiClient dashboard. Select the AV tab on the left pane. Then click the settings icon on Real-Time Protection in the right pane.

The following may be selected on the AV settings page:

- File scanning (previously, Real-Time Protection or RTP)
- Malicious website detection
- Botnet detection (block known communication channels)

FortiClient Banner Design

If FortiClient is running in standalone mode and not registered to a FortiGate or EMS, a single banner at the bottom of the GUI is displayed. This is true for both the FortiClient full version, as well as the VPN only version. When registered to a FortiGate or EMS, the banner is hidden by default. Similarly, when created from a FortiClient Configurator, no banner is displayed by default.

Logging

Enhancement to FortiClient Logs

FortiClient will create a log entry to show just the URL visited by the user through a web browser. This is in addition to the network level logs generated by FortiClient.

Installation Information

Firmware images and tools

When installing FortiClient version 5.4.0, you can choose the setup type that best suits your needs. You can select one of the two options:

- Complete: all Endpoint Security and VPN components will be installed.
- VPN Only: only VPN components (IPsec and SSL) will be installed.

FortiClient includes various tools to help with and customize installations. The following tools and files are available in the *FortiClientTools* file:

- *OnlineInstaller*: downloads and installs the latest FortiClient file from the public FortiGuard Distribution Server (FDS).
- *FortiClientConfigurator*: an installer repackaging tool that can be used to create custom installation packages
- *RebrandingResources*: resources used by the FortiClient Configurator tool for rebranding.

When creating a custom FortiClient 5.4.0 installer using the FortiClient Configurator tool, you can choose which features to install. You can also enable or disable software updates, configure SSO, and rebrand FortiClient .

Upgrade from a previous version

FortiClient version 5.4.0 supports upgrading from FortiClient 5.2.0 or later.

Please review the Introduction and Product Integration and Support chapters prior to installing FortiClient version 5.4.0.

Downgrade to previous versions

Downgrading FortiClient version 5.4.0 to previous FortiClient versions is not supported.

Uninstall FortiClient

To uninstall FortiClient version 5.4.0, use the *Application* > *FortiClient* > *Uninstaller* application.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at https://support.fortinet.com. After logging in, click on *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiClient 5.4.0 support

The following table lists FortiClient (Mac OS X) 5.4.0 product integration and support information.

Desktop Operating Systems	• Mac OS X v10.8 Mountain Lion • Mac OS X v10.9 Mavericks • Mac OS X v10.10 Yosemite • Mac OS X v10.11 El Capitan
Minimum System Requirements	• Intel processor • 256MB of RAM • 20MB of hard disk drive (HDD) space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for FortiClient documentation
FortiAnalyzer	• 5.0.2 and later • 5.2.0 and later • 5.4.0
FortiAuthenticator	• 2.2.0 and later • 3.0.0 and later • 3.1.0 and later • 3.2.0 and later
FortiManager	• 5.0.2 and later • 5.2.0 and later • 5.4.0
FortiOS	• 5.0.0 and later • 5.2.0 and later • 5.4.0 Some FortiClient features are dependent on specific FortiOS versions.

Language support

The following table lists FortiClient language support information.

Language	GUI	XML Configuration	Documentation
English	✓	✓	✓
Chinese (Simplified)	✓		
Chinese (Traditional)	✓		
French (France)	✓		
German	✓		
Japanese	✓		
Korean	✓		
Portuguese (Brazil)	✓		
Russian	✓		
Spanish (Spain)	✓		

The FortiClient language setting defaults to the regional language setting configured on the client workstation unless configured in the XML configuration file.

If the client workstation is configured to a regional language setting that is not supported by FortiClient , it defaults to English.

Resolved Issues

The following issues have been fixed in FortiClient (Mac OS X) 5.4.0. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
202465	Virus trigger causes Microsoft Outlook to stop working and Database corruption occurs.
266830	Unable to see quarantine files in FortiClient.
267147	FortiClient on Mac OS Yosemite does not use the system proxy settings.
272551	When FortiGate language is set to Japanese and the split tunnel is configured, users cannot connect SSLVPN to the FortiGate.
279443	Web Filter not blocking `https`.
281556	Update OpenSSL libraries to version 1.0.2b.
282297	FortiClient Mac custom package with partial config does not register to FortiGate.
284559	Update `sqlite` source code to `3.8.10.2`.
284836	Update OpenSSL library to `v1.0.2d`.

Known Issues

The following issues have been identified in FortiClient (Mac OS X) 5.4.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
271427	Host CPU may increase when using the `type ahead` feature in Eclipse Luna on Mac OS when FortiClient is registered on FortiGate.
291465	Software update is displayed even when disabled.
294213	DNS traffic may stop working with SSL VPN split tunnel on Mac OS X 10.11. Network traffic requiring use of the local DNS is blocked in the following conditions: • SSL VPN split tunnel • Mac OS X 10.11 - El Capitan • DNS configured on FortiGate • DNS IP address goes through the FortiGate **Workaround:**Use a public DNS or use full tunnel
309575	Network traffic may stop working after IPsec VPN connection is established . **Workaround:** is to disable both Application Firewall and Web Filtering.
298065	FortiClient may cause random system crashes and reboots on Mac OS X El-Capitan.